APPARATUS AND METHODS FOR QUANTUM KEY DISTRIBUTION

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a bypass continuation application of International Application No. PCT/US2016/034639, filed May 27, 2016, and entitled "Apparatus and Methods for Quantum Key Distribution," which claims the priority benefit of U.S. Application No. 62/167,515, filed May 28, 2015, and entitled "MEASUREMENT-DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION BASED ON PHOTONIC INTEGRATED CIRCUITS." Each of these applications is hereby incorporated herein by reference in its entirety.

BACKGROUND

[0002] Measurement-device-independent quantum key distribution (MDI-QKD) is a method of distributing secret keys that can be immune to detector side channel attacks. The scheme includes at least two sending chips (usually referred to as Alice and Bob), which encode signals in single photons through either time-bin encoding or polarization encoding, as well as a receiver chip (usually referred to as Charlie), which measures the signals in the maximally-entangled Bell basis.

[0003] To implement the MDI-QKD protocol, Alice and Bob randomly and independently prepare photon signals in one of the four BB84 states: $|0\rangle$, $|1\rangle$ in the Z-basis, or $|+\rangle$, $|-\rangle$ in the X-basis. These photons are then sent via the quantum channel to Charlie who is instructed to perform a Bell state measurement. The four Bell states are summarized in Table 1. Alice and Bob can also apply the decoy state protocol to their photon signals to estimate the gain (i.e., the probability that Alice and Bob's signals yield a successful Bell measurement) and the quantum bit error rate (QBER, the rate of false successful Bell measurements due to single photon contributions).

[0004] Charlie announces whether or not his Bell state measurements are successful along with the Bell state obtained. Alice and Bob retain only the data that correspond to successful Bell state measurements and discard the rest. For the data they retained, Alice and Bob each reveal their basis choices over the public channel and retain only those instances where they chose the same basis. Bob then flips parts of his data to directly correlate his measurements with those of Alice. Finally, Alice and Bob apply error correction and privacy amplification to establish identical secret keys.

TABLE 1

The four Bell states and possible bit flips to directly correlate Alice and Bob's bits

	Bell state reported by Charlie			
Basis chosen by Alice and Bob	$\|\psi^-\rangle$ = $(\|01\rangle - \|10\rangle)/\sqrt{2}$	$\|\psi^+\rangle$ = $(\|01\rangle + \|10\rangle)/\sqrt{2}$	$\|\phi^-\rangle$ = $(\|00\rangle - \|11\rangle)/\sqrt{2}$	$\|\phi^+\rangle$ = $(\|00\rangle + \|11\rangle)/\sqrt{2}$
Z basis	Flip	Flip	—	—
X basis	Flip	—	Flip	—

[0005] The rate of secret key generation (in bits per second, per Bell state), in the limit of large number of signals exchanged for each Bell state $|k\rangle \epsilon \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ is

$$R_{|k\rangle} \geq r\left\{Q\frac{1,1}{z,|k\rangle}\left[1 - H_2\left(e\frac{1,1}{x,|k\rangle}\right)\right] - Q\frac{vsa,vsb}{z,|k\rangle}fe\left(E\frac{vsa,vsb}{z,|k\rangle}\right)\left(H_2\frac{vsa,vsb}{z,|k\rangle}\right)\right\} \quad (1)$$

where r is the repetition rate in Hz

$$Q\frac{1,1}{z,|k\rangle} \text{ and } \frac{1,1}{x,|k\rangle}$$

are the gain and QBER due to single photon signals;

$$Q\frac{vsa,vsb}{z,|k\rangle} \text{ and } e\frac{1,1}{x,|k\rangle}$$

are the gain and QBER for signals emitted by Alice and Bob with mean photon number V_{sa} and V_{sb}, respectively; $fe \geq 1$ is the error correction inefficiency; $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. The equation for the secret key generation rate assumes that Alice and Bob use the Z-basis for key generation and only use the X-basis for security checks. The quantities

$$Q\frac{vsa,vsb}{z,|k\rangle} \text{ and } E\frac{vsa,vsb}{z,|k\rangle}$$

can be measured directly as the MDI-QKD system is run, while the quantities

$$Q\frac{1,1}{z,|k\rangle} \text{ and } e\frac{1,1}{x,|k\rangle}$$

can be measured using the decoy-state protocol.

[0006] A more detailed description of the protocol with two decoy states is as follows. The protocol can be performed with more than two decoy states, but in practice it can be desirable to have as few decoy states as possible. The first four steps of the protocol—state preparation, state distribution, Bell state measurement, and sifting—are repeated N times until the successful sifting conditions are met.

[0007] Step 1: State preparation. Alice and Bob randomly and independently choose an intensity for their photon signals: $V_a \epsilon \{V_{sa}, V_{da,1}, V_{da,2}\}$ for Alice and $V_b \epsilon \{V_{sb}, V_{db,1}, V_{db,2}\}$ for Bob. $V_{sa}(V_{sb})$ corresponds to the intensity of the signal state for Alice (Bob) and $V_{da,i}$, $(V_{db,i})$ for 1,2 corresponds to the intensity of the decoy states for Alice (Bob). The two decoy states typically have weaker intensities than the signal state. Alice and Bob then randomly and independently choose a basis $B_i \epsilon \{Z,X\}$, and a bit $r_i \epsilon \{0,1\}$ with